

OPTENET Security Suite PC

Versión 10.09.39



COPYRIGHT

Queda prohibida la reproducción, transmisión, transcripción, almacenamiento en sistemas de recuperación y traducción a cualquier idioma de esta publicación, independientemente de cuál sea la forma o el medio, sin el consentimiento expreso por escrito de OPTENET S.A. o de sus proveedores o empresas afiliadas.

ATRIBUCIÓN DE MARCAS COMERCIALES

OPTENET, EDUNET, COTENET, E-OPTENET, OPTENET.BE, OPTENET.CL, OPTENET.CO.CR, OPTENET.COM.EC, EDUNET.COM.ES, OPTENET.COM.ES, EDUNET.ES, OPTENET.ES, OPTENET.US, OPTENET.FR, OBTENET.COM, OBTENET.NET, OPTENET.COM, OPTENET.NET, CAPITANNET.COM, CAPITANNET.ORG, CAPITANNET.NET, CAPITANET.COM, CAPITANET.ORG, CAPITANET.NET, OPTENET.BIZ, PROTEGELES.COM, PROTEGELES.NET, PROTEGELES.ORG, SURF-MATE.COM, SURF-MATE.NET, SURF-MATE.ORG, PROTEGELOS.COM, PROTEGEALOSNINOS.COM, SIFT-PLATFORM.ORG, OPTENET.COM.GT, OPTENET.COM.HN, OPTENET.COM.MX, OPTENET.COM.PA, OPTENET.COM.PE, PTENET.CO.UK (en trámite), optenet.com.ve, son marcas comerciales registradas o marcas comerciales de OPTENET S.A. y/o sus afiliados en España y/o en otros países. Las demás marcas comerciales registradas o sin registrar aquí mencionadas son propiedad exclusiva de sus respectivos propietarios.

INFORMACIÓN DE LICENCIA

ACUERDO DE LICENCIA

AVISO A TODOS LOS USUARIOS: LEA ATENTAMENTE EL ACUERDO JURÍDICO APROPIADO CORRESPONDIENTE A LA LICENCIA QUE HA ADQUIRIDO. EN ÉL SE EXPONEN LOS TÉRMINOS Y CONDICIONES GENERALES QUE RIGEN EL USO DEL SOFTWARE CON LICENCIA.

ÍNDICE





1 INTRODUCCIÓN

1.1 OPTENET Security Suite

OPTENET Security Suite es una herramienta que le permite optimizar el uso de Internet, al mismo tiempo que le ofrece las mejores garantías de seguridad. Ofrece la protección más eficaz existente en el mercado tanto para los equipos informáticos como para los usuarios de los mismos.

Esto se logra tanto por la gran eficacia de sus componentes particulares como por la óptima combinación de los mismos.

Asimismo, OPTENET Security Suite es una aplicación transparente que no afecta al funcionamiento de las demás aplicaciones existentes, ni al rendimiento de los equipos informáticos, ni a la velocidad de las comunicaciones.

1.2 Filtro Web de Contenidos de OPTENET Security Suite

El Filtro de contenidos es un software de fácil instalación que permite evitar el acceso a contenidos no deseados de Internet, como sitios pornográficos, descarga de archivos peligrosos, servidores de mensajería instantánea, P2P, etc.

El Filtro de contenidos es responsable de capturar el tráfico que entra y sale del PC. Además de identificar el tipo de tráfico, solicita al servicio integrado correspondiente que analice, monitorice o rastree el contenido, de modo que pueda garantizar al usuario una navegación segura en función de los parámetros configurados.

Se basa en el análisis semántico de contenidos de sitios web y listas de sitios clasificados en diversas categorías de contenido. Las listas se actualizan cada diez minutos. El análisis semántico verifica, independientemente de si el sitio pertenece o no a la lista, si éste posee algún texto de contenido inapropiado, en cuyo caso se bloqueará para el usuario.

1.3 Filtrado de Protocolos

El filtrado de protocolos detecta conexiones e identifica el tipo de protocolo, realizando diferentes acciones en función de la configuración. De esta forma, los usuarios pueden controlar aplicaciones como la mensajería instantánea, los programas P2P, el chat, el correo electrónico y los grupos de noticias.

1.4 Idiomas de OPTENET Security Suite

OPTENET Security Suite filtra los principales idiomas utilizados en Internet con una eficacia superior al 98%. Las listas de Security Suite contienen páginas de todos los idiomas. Además, el analizador semántico se entrena periódicamente con páginas de todo el mundo, lo que le permite detectar páginas en todo tipo de idiomas.

Para alcanzar el grado de eficiencia máximo (99%), en determinadas áreas geográficas se establece un conjunto de páginas suficientemente amplio para el entrenamiento del analizador semántico, como por ejemplo en español, inglés, francés, holandés, portugués, alemán e italiano.

1.5 Velocidad de Navegación en Internet usando OPTENET Security Suite

La Suite de Seguridad es extremadamente rápido y, por lo tanto, imperceptible desde el punto de vista del usuario. Tanto la consulta de las listas como el proceso de análisis de contenido realizados por el sistema tardan una milésima de segundo. Se trata de una consulta inmediata.

1.6 Seguridad del filtro Web de contenidos

Si alguien intenta burlar el filtro, el acceso a Internet se bloqueará completamente como medida de protección. Sólo es posible restablecer el acceso utilizando una contraseña.

1.7 Servicio de desbloqueo de Páginas bloqueadas por error

Security Suite posee un margen de error de cerca del 0,1%, el más bajo del mercado. Además, dispone de un servicio de desbloqueo. Si una página se bloquea por error, el usuario puede enviar automáticamente un correo electrónico dirigido a nuestro Centro de Atención al Cliente (CAC) exponiendo el motivo del error para su corrección. El usuario volverá a tener acceso a esa página en 15 minutos aproximadamente.

1.8 Activación o Desactivación de la Security Suite

Security Suite se activa o desactiva mediante una contraseña para que los administradores puedan navegar sin restricciones. La contraseña se le solicita al usuario en el momento de la instalación. En caso de que no se disponga de la contraseña, o si alguien intenta desactivar Security Suite, el sistema dispone de mecanismos de autoprotección para que sea imposible desactivarlo.

1.9 Bloqueo de Programas de intercambio y descarga de archives P2P

Es posible bloquear los programas de intercambio y la descarga de archivos P2P dentro de la configuración de protocolo del Filtro de contenidos. La categoría de servidores P2P también puede bloquearse, ofreciendo así un mayor nivel de eficacia.

1.10 Bloqueo de Programas de mensajería Instantánea

Es posible bloquear los programas de mensajería instantánea dentro de la configuración de protocolo del Filtro de contenidos. La categoría de servidores de mensajería instantánea también puede bloquearse para ofrecer un mayor nivel de eficacia.

1.11Actualizaciones

El sistema se actualiza automáticamente a través de Internet. Este proceso no requiere administración.





2 REQUISITOS TÉCNICOS

2.1 Conocimientos Técnicos

El programa ha sido diseñado para que pueda ser instalado sin problemas por usuarios con conocimientos básicos de informática.

2.2 Compatibilidad de Sistemas

La OSSPC está disponible para los siguientes Sistemas Operativos:

- Windows XP Sp2
- Windows Vista (32 and 64 bits)
- Windows 7 (32 and 64 bits)

Sistema Operativo	RAM. Mínimo	Espacio libre en Disco:
Windows XP sp2	512 MB	200 MB
Windows Vista 32 bits, 64 bits	1 GB	200 MB
Windows 7 32 bits	1 GB	200 MB
Windows 7 64 bits	2 GB	200 MB

Puede ser utilizado con cualquier navegador web.



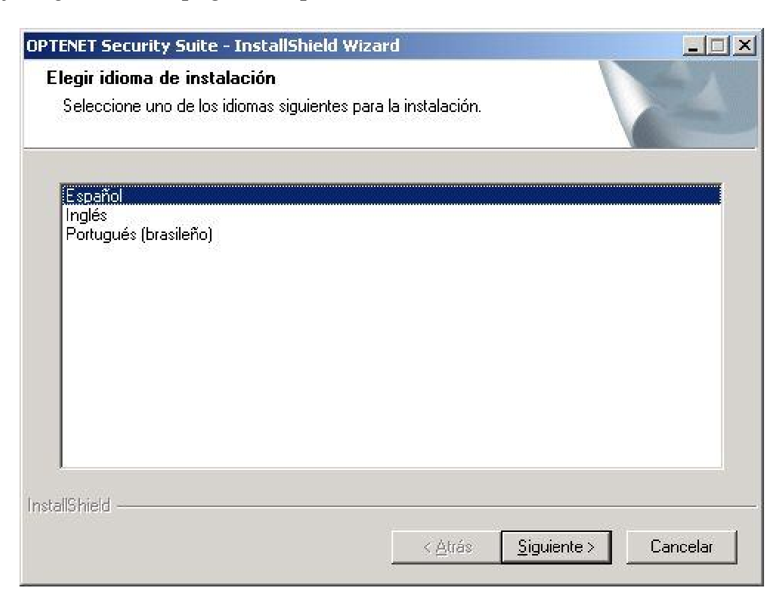


3 INSTALACIÓN

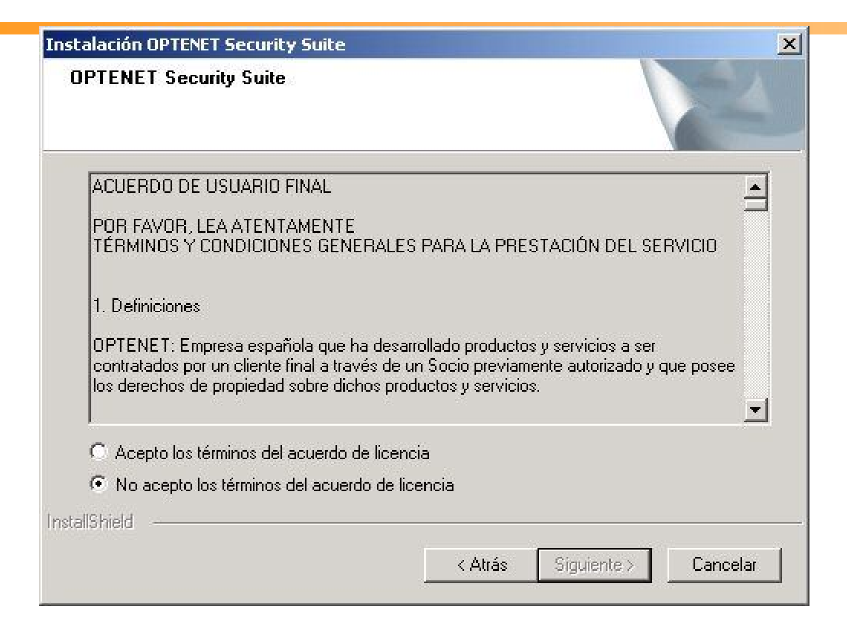
Tanto si descarga la aplicación desde una página web, como si lo va a instalar desde un CD, le recomendamos que guarde el programa en el disco duro del PC y siga estos pasos:

1) Haga doble dick en el archivo ejecutable de Optenet (tendrá un nombre similar a OptenetSecuritySuite.exe)

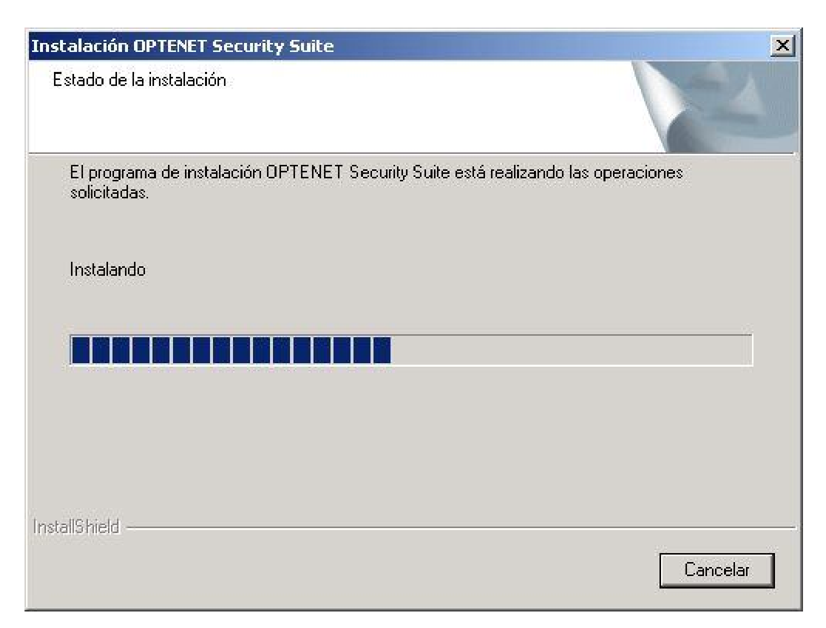
2) La interfaz de OPTENET está disponible en tres idiomas: español, inglés y portugués. Seleccione el idioma y haga click en [*Siguiente*].



3) Aceptación de Licencia de Usuario final. Lea y Acepte los términos de la licencia:



4) La instalación comenzará:



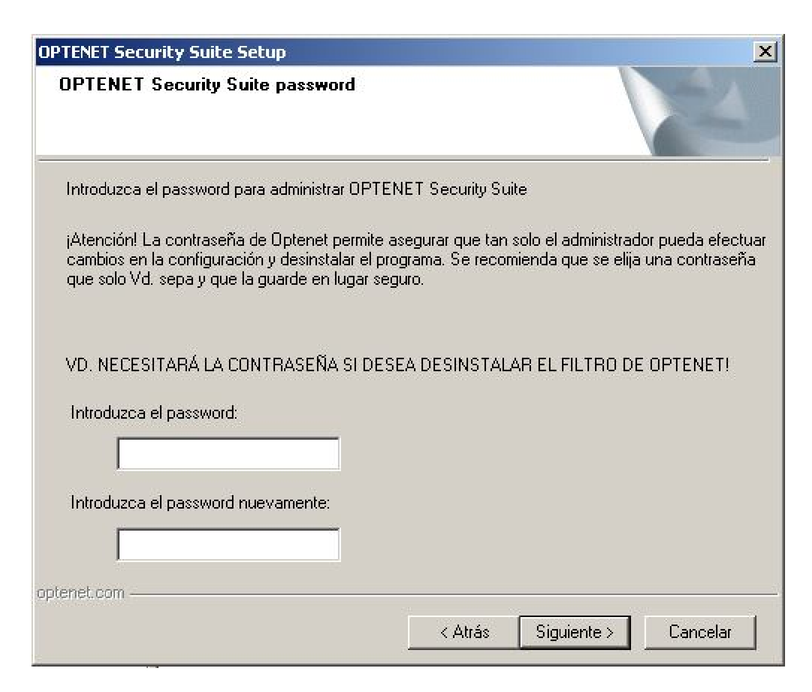
5) Seleccione el directorio en el que instalar el software. Por defecto se utilizará el directorio de "Archivos de Programa". Haga Click en [*Siguiente*].



6) Introduzca la Contraseña a utilizar para accede a la Consola de Administración de la Suite de Optenet (para la configuración del filtro).

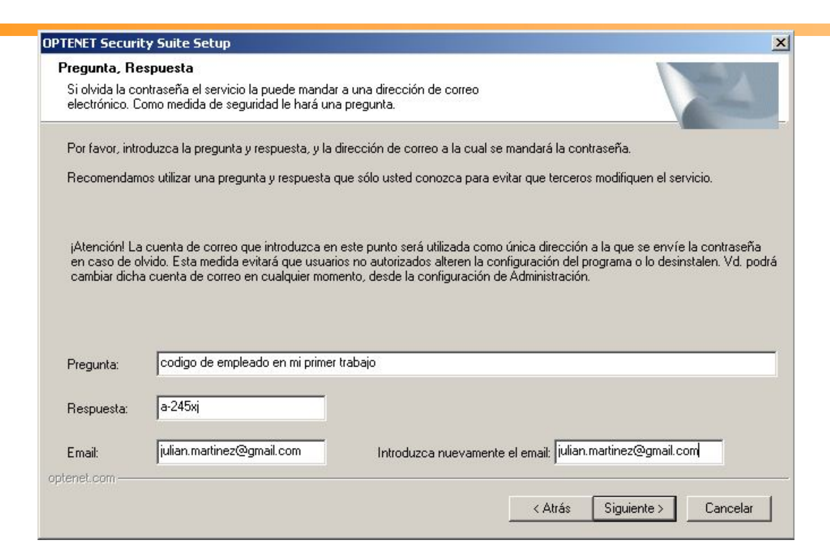
Esta Contraseña asegura que tan solo el administrador pueda efectuar cambios de configuración o desinstalar el programa. Se recomienda que elija una Contraseña que tan solo Vd. Conozca y que la guarde en lugar seguro.

⚠ Recuerde que esta contraseña será solicitada si en el futuro desea desinstalar la Suite de OPTENET.



7) Recordatorio de Contraseña:

- Introduzca una pregunta y respuesta de control, a ser utilizadas en caso de que olvide la contraseña.
- Introduzca una cuenta de correo a la que enviar la Contraseña en caso de que tampoco recuerde la respuesta a la pregunta introducida en este apartado. ⚠ ¡La cuenta de correo introducida en este apartado será la única a la que la contraseña sea enviada en caso de que la haya olvidado! – Esta medida evitará que Usuarios no autorizados adquieran la Contraseña de Administración a fin de modificar la configuración del filtro y/o desinstalar el programa.



8) Introduzca el código de Licencia (probablemente recibido vía correo electrónico tras haber comprador el producto).

(Donde esté disponible) También podría ser posible el uso de una licencia de evaluación que permita probar otros Productos de OPTENET (suite completa etc.). En este caso, seleccione de Producto de Evaluación a instalar y haga click sobre el botón [*Siguiente*].

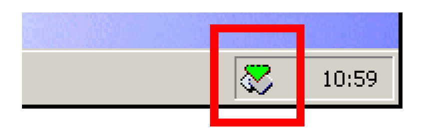


9) Finalmente, es altamente recomendable que reinicie su PC para completar la instalación.

El programa podría no funcionar correctamente hasta que el PC sea reiniciado.



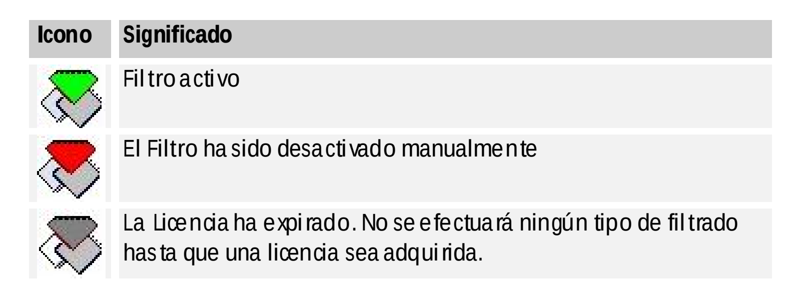
10) Una vez que el PC haya sido reiniciado, nótese que un nuevo icono es mostrado en la barra de estado de Windows.



Haga click con el botón derecho del ratón sobre este icono para abrir el menú contextual (las opciones listadas podrían variar dependiendo del producto instalado):



Este icono además variará en color, indicado el estado del filtro u operaciones adicionales que se estén llevando a cabo en un momento dado:



Icono	Significado
	Filtro activo
	El Filtro ha sido desactivado manualmente
	La Licencia ha expirado. No se efectuará ningún tipo de filtrado hasta que una licencia sea adquirida.





4 CONFIGURACIÓN

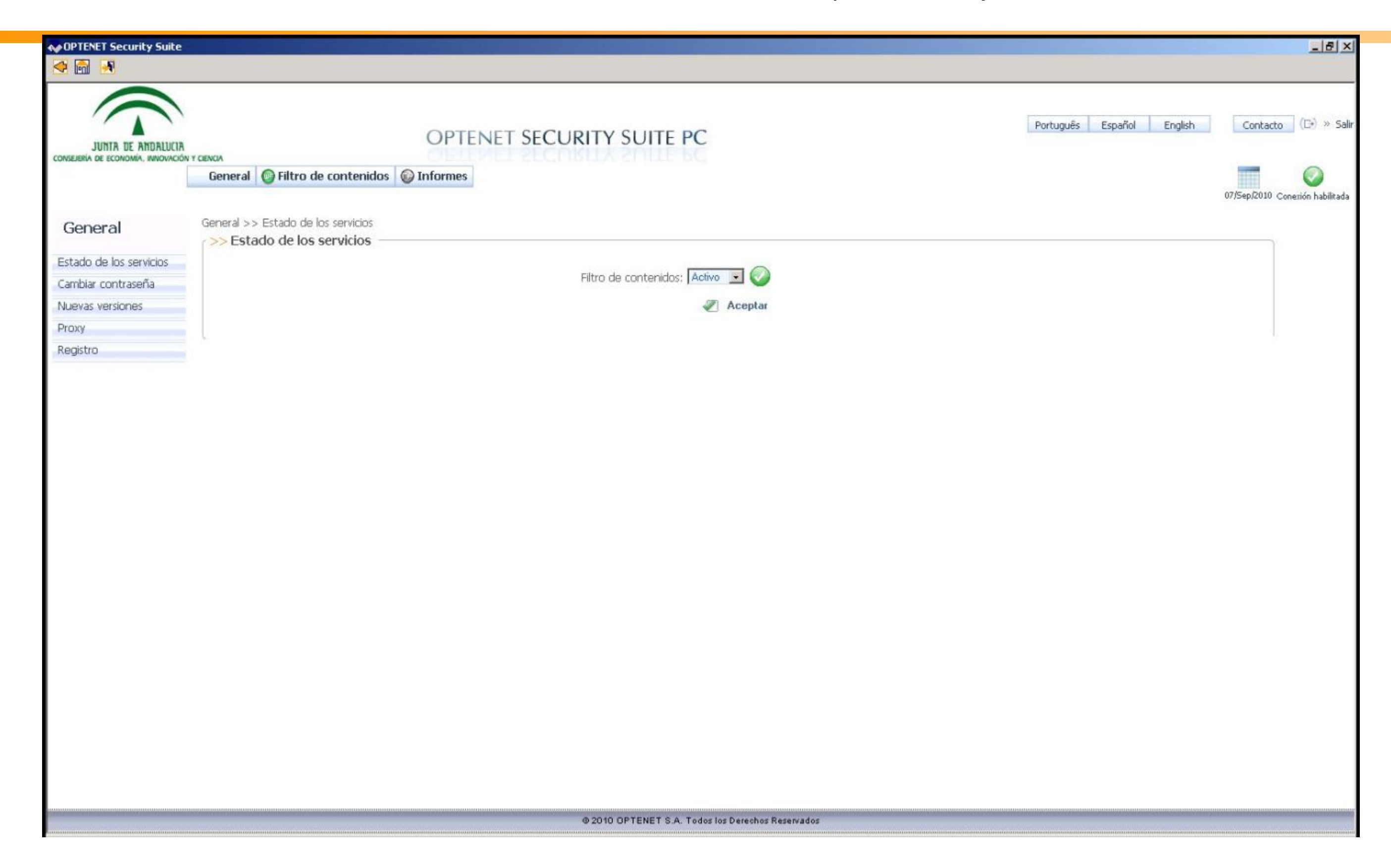
Vd. podrá acceder a la Consola de OPTENET Security Suite:

- Desde un menú accesible desde el botón [*Inicio*] de Windows.
- O bien, haciendo click con el botón derecho del ratón sobre el icono situado en la barra de estado de Windows, seleccionado la opción del menú desplegable [Administración de Optenet Security Suite].

La contraseña de administración será requerida para evitar el acceso no autorizado (la contraseña indicada en el momento de la instalación del Software).



Una vez haya introducido correctamente la contraseña, se mostrará la consola de Administración:



La suite de Seguridad de OPTENET está clasificada en las siguientes secciones (acorde a disponibilidad y siempre en base al producto bajo licencia):

- General
- Filtro de Contenidos
- Informes



5 GENERAL

Esta sección proporciona información sobre la herramienta y los servicios incluidos, permitiendo efectuar tareas de configuración de carácter general como:

- Habilitar/deshabilitar el Servicio de Filtrado.
- Cambio de la Contraseña de Administración.
- Configuración de la actualización del Software.
- Cambio del Código de Licencia, configuración del proxy de salida a internet (en caso de ser preciso) etc.

Al hacer click sobre la pestaña [*General*], el siguiente menú será mostrado a la izquierda de la consola:



5.1 Estado del Servicio

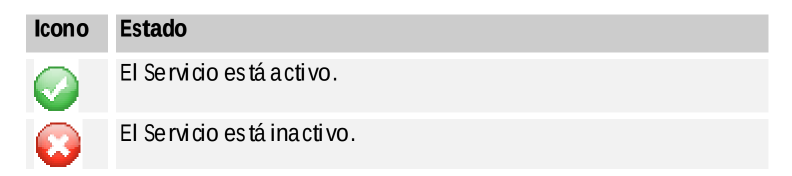
La Suite de Seguridad de OPTENET para la Junta de Andalucia incluye el servicio:

- Filtro de Contenidos (control parental),

En esta sección, podrá activarlo o desactivarlo:



Existirá una lista desplegable que permitirá la activación/desactivación independiente de los Servicios de filtrado. Un icono diferenciado indicará si el Servicio está activo o no actualmente. En caso de que un Servicio no esté activo, no serán aplicadas las restricciones establecidas.



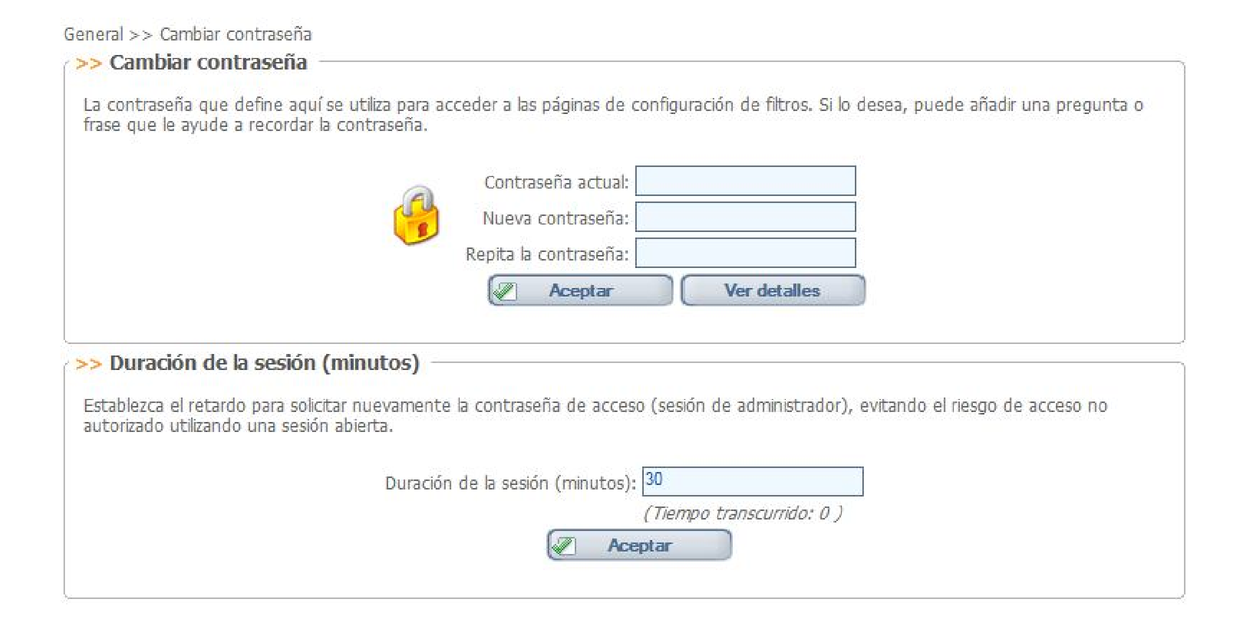
Icono	Estado
	El Servicio está activo.
	El Servicio está inactivo.

Recuerde hacer click sobre el botón [*Aceptar*] para aplicar los cambios efectuados.

5.2 Cambiar Contraseña

Esta sección permitirá:

- El cambio de la Contraseña de Administración.
- El cambio de la Pregunta/Respuesta de control (a ser utilizadas en caso de que olvide la Contraseña de Administración).
- El establecimiento de la duración de la Sesión.



5.2.1 Cambio de la Contraseña de Administración

Es decir, la contraseña que permite el acceso a la administración de la Suite de Optenet que fue introducida por primera vez durante la instalación del Producto.



Recuerde que esta Contraseña evita el acceso no autorizado de forma que la configuración solo pueda ser efectuada por el administrador.

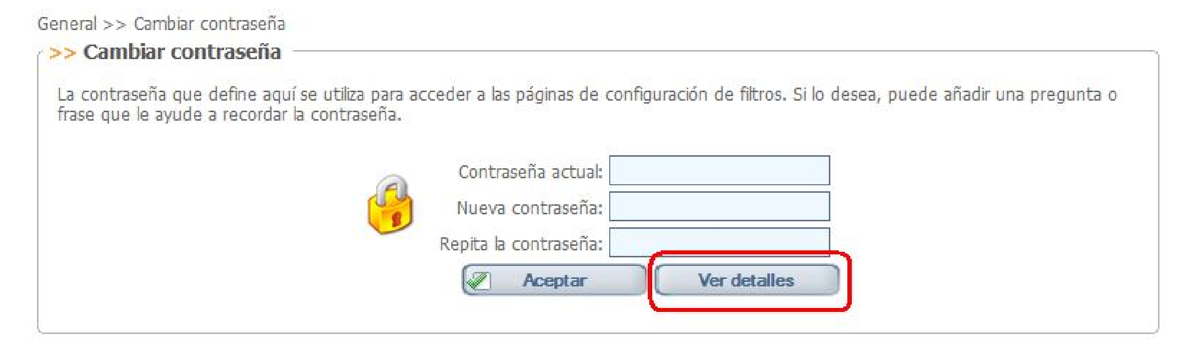
A fin de cambiar la Contraseña:

- Introduzca su Contraseña actual.
- Introduzca la nueva Contraseña (y confírmela introduciéndola nuevamente).

Como medida de seguridad adicional, en caso de que la consola de administración permanezca abierta durante un largo periodo, se solicitará la re-introducción de la contraseña de forma periódica (por defecto, cada 30 minutos). Esta medida evita el riesgo de dejar por olvido la Consola de Administración abierta permitiendo que usuarios no autorizados puedan cambiar la configuración sin su conocimiento.

Introduzca el tiempo de vida de la sesión (periodo de tiempo antes de volver a solicitar la introducción de la Contraseña para continuar operando con la Consola de Administración). El tiempo vendrá expresado en minutos.

5.2.2 Cambio de la Pregunta/Respuesta de Recuperación de Contraseña y la dirección de Correo



Desde la ventana [*Cambiar Contraseña*], haga click en el botón [*Ver Detalles*]. Se mostrará una nueva ventana en la que se podrá cambiar:

- La Pregunta / Respuesta de Seguridad. ⚠ Obsérvese que la respuesta es sensible a mayúsculas / minúsculas.

  y/o

- La dirección de Correo.

General >> Cambiar contraseña >> Ver detalles

>> Ver detalles

-Si olvida su contraseña, aparecerá esta pregunta y, si proporciona la respuesta correcta, se le enviará la contraseña a la dirección de correo electrónico que especifique aquí.
Por ejemplo, podría especificar la pregunta "¿Cuál es el nombre de mi gato?", con la respuesta "Félix". La respuesta distingue entre mayúsculas y minúsculas: Félix no es lo mismo que félix, fÉlix etc.
Tenga en cuenta también que esta pregunta se mostrará a cualquier que intente (sin éxito) acceder a las páginas de configuración. Por este motivo, debe elegir una pregunta de la que sólo usted conozca la respuesta.-

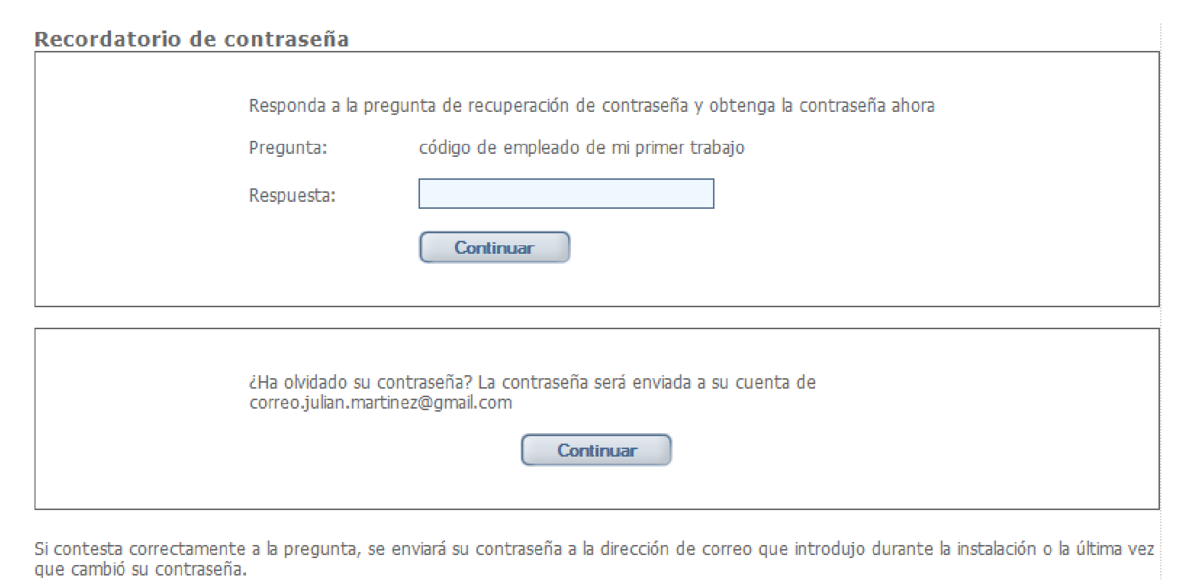
Frase o pregunta: código de empleado de mi prim
Respuesta: a-245xj
Correo electrónico: julian.martinez@gmail.com

Aceptar Volver

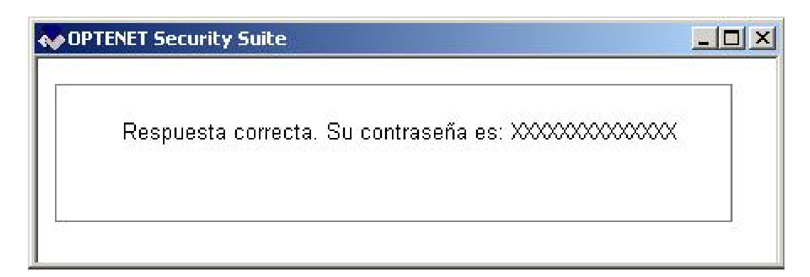
Una vez haya guardado estos cambios, en caso de haber olvidado la Contraseña de Administración y haberla olvidado, tan solo será preciso hacer click en el enlace que aparece en la parte inferior de la ventana:



Se mostrará una ventana en la que se solicita la respuesta a la pregunta de Seguridad:



- En caso de respuesta correcta, la contraseña será mostrada por pantalla:



- Si no recuerda la respuesta, siempre podrá solicitar que le sea enviada a la cuenta de correo que haya configurado.

5.3 Nuevas Versiones (Actualización de Software)

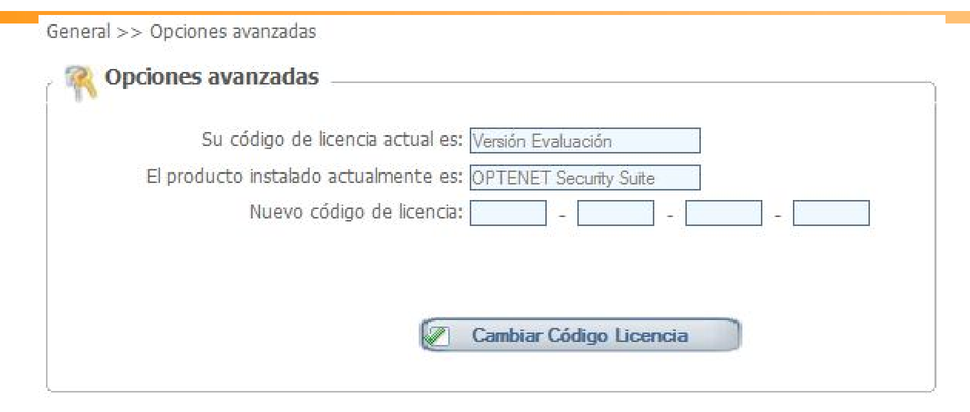
OPTENET Security Suite puede actualizarse automáticamente de forma que Vd. no tendrá que preocuparse por nuevas versiones. Si no se configuran las actualizaciones automáticas, OPTENET Security Suite notificará de la disponibilidad de nuevas versiones. También será posible la actualización del Software bajo petición explícita del usuario en tiempo real.

Seleccione asimismo el tipo de alerta a ser utilizada cuando una nueva versión esté disponible.



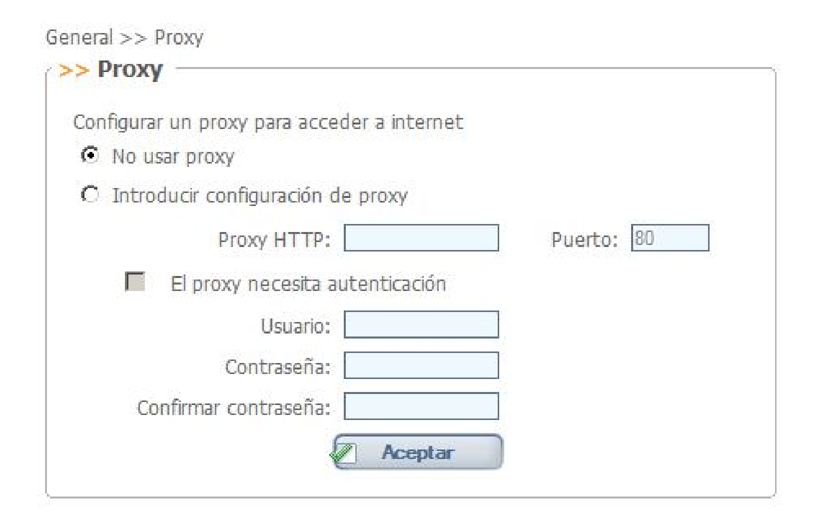
5.4 Opciones Avanzadas

Esta sección permitirá el cambio del código de licencia asociado a la Suite.



5.5 Configuración del Proxy

En caso de no contar con una conexión directa a Internet, esta sección le permitirá la configuración del proxy. Si el uso del proxy requiere autenticación, introduzca el usuario / Contraseña a ser utilizado.







6 FILTRO DE CONTENIDOS WEB

Esta sección permitirá la configuración del comportamiento de la herramienta en lo relativo al filtrado web (restringir el acceso a sitios web de contenido inapropiado, la descarga de ciertos tipos de ficheros etc.).

Al hacer click sobre la pestaña [Filtro de Contenidos], el siguiente menú será mostrado a la izquierda:



6.1 Configuración

Desde la opción de Configuración del Filtro de Contenidos, es sencillo indicar qué tipo de contenidos estarán accesibles para los usuarios.

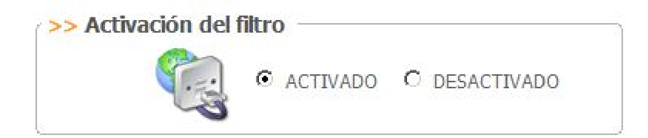
La ventana estará dividida en secciones diferenciadas:

- Activación del Filtro
- Bloqueo de Acceso a Internet por acceso reiterado a páginas prohibidas
- Categorías a filtrar
- SafeSearch (Búsqueda Segura).
- Tipos de Archivos a filtrar
- Horarios de Navegación



6.1.1 Estado del Filtro: Activado / Desactivado

Vd. podrá activar o desactivar el filtro a su voluntad:



- Desactivado: Los usuarios podrá acceder a Internet sin ningún tipo de limitación.
- Activado: Se restringirá el acceso a las categorías de sitios web que se indiquen y la descarga de los tipos de ficheros que se especifiquen.

6.1.2 Bloqueo de Internet por acceso reiterado a páginas prohibidas



Será posible el bloqueo del acceso a internet para aquellos usuarios que intenten acceder a 10 páginas prohibidas durante la misma sesión de navegación. Marque la Casilla de verificación para activar esta funcionalidad.

- Tan solo el usuario que ha intentado el acceso a las páginas prohibidas es bloqueado (no el resto de potenciales usuarios del PC).
- Para posibilitar que el usuario navegue de nuevo, haga click sobre el botón [*Desbloquear*].
- Será posible configurar una cuenta de correo en la que se reciban notificaciones cada vez que un usuario ha sido bloqueado por la aplicación de esta política. La notificación recibida en el correo indicará el usuario que ha sido bloqueado.

6.1.3 Seleccionando las Categorías Web a bloquear

Seleccione las Categorías a bloquear: Las páginas web que hayan sido clasificadas bajo esas categorías serán bloqueadas.

Por defecto, algunas categorías ya habrán sido marcadas:



>> Categorías para filtrar

☐ Alcohol y tabaco	☐ Almacenamiento en linea	☑ Anonimizadores	☑ Anorexia y bulimia
☐ Azar	☐ Banners	☑ Bombas	☐ Chat
☐ Compras	☐ Correo web	☑ Drogas	☐ Encuentros
☐ Foros	☐ Fotos y videos	☐ Hackers	☐ Juegos
☐ Juegos adultos	☐ Mensajeria instantanea	☐ Modelos	☐ Musica
☐ Paginas personales	☑ Pornografia	☑ Racismo	☐ Radio y tv en linea
☐ Redes sociales	☐ Rosa	☑ Sectas	☐ Servidores p2p
☐ Sexualidad	☐ Spyware	☑ violencia	

Alcohol y tabaco: sitios web que venden y/o promueven el uso de tabaco y alcohol para consumo humano, así como productos directamente relacionados con su ingesta.

Juegos de azar: sitios web que permiten el acceso a casinos y salas de bingo por Internet, así como a concursos basados en SMS. Esta categoría incluye sitios web en los que pueden realizarse todo tipo de apuestas y también los que ofrecen instrucciones para jugar o que promueven activamente este tipo de actividades

Compras: sitios web a través de las cuales pueden realizarse compras de diversos productos y servicios. Sitios que permiten la compraventa entre particulares o entre empresas y particulares. Se incluyen las ofertas de vehículos e inmobiliaria, incluso si las transacciones no se realizan directamente. No incluye apuestas, viajes ni instituciones financieras.

Foros: sitios web de carácter temático donde se puede participar aportando opiniones personales.

Juegos para adultos: sitios con juegos de naturaleza violenta, erótica o pornográfica; también juegos con temáticas racistas, sectarias y discriminatorias. Incluye los juegos abiertos multijugador en los que la acción puede derivar hacia los contenidos mencionados.

Sitios web personales: sitios web personales creados por usuarios de todo el mundo para presentarse a sí mismos o presentar determinados temas de su interés.

Redes sociales: sitios web específicamente diseñados al establecimiento de comunidades en línea, en las que los usuarios comparten información entre sí. Estos sitios pueden tener propósitos profesionales o de ocio. No se incluyen los sitios dedicados a relaciones y a contactos entre adultos.

Sexualidad: Información y artículos sobre sexo, educación sexual, tendencias sexuales, etc., que no contienen pornografía.

Almacenamiento en línea: sitios web que ofrecen a los usuarios la posibilidad de almacenar en línea un gran número de archivos, ya sea con el objeto de compartirlos como para uso personal. No incluye P2P.

Banners: banners de publicidad insertados en páginas web. Incluyen los sitios que los sirven.

Correo web: sitios web a los que pueden enviarse y en los que pueden recibirse mensajes de correo electrónico.

Fotos y vídeos: sitios web que alojan y permiten la publicación y visionado de imágenes y vídeos. Esta categoría no incluye la fotografía artística y profesional.

Servidores de mensajería instantánea: sitios web desde los que pueden descargarse programas. Incluye sitios web que permiten el envío de SMS desde Internet.

Pornografía: sitios web con contenidos pornográficos u obscenos. Esta categoría incluye el acceso a los chats en los que puede encontrarse este tipo de materiales.

Rosa: sitios web con contenidos relativos a famosos; además, contenidos como moda, decoración, etc.

Software espía: Sitios web que contienen software espía (spyware). El software espía es un programa que recoge información de un PC y la transmite a fuentes externas a través de Internet. Todo esto tiene lugar sin el conocimiento o la autorización del propietario del ordenador.

Anonimizadores: sitios web que permiten a los usuarios navegar por Internet y acceder a contenidos sin quedar registrados por terceros.

Bombas (y armas): Páginas web que explican cómo preparar, construir, distribuir y utilizar explosivos y artefactos explosivos. También sitios de información, promoción o venta de armas de fuego y armas blancas sea para uso militar, deportivo o caza. No se incluyen en esta categoría los cuchillos de bolsillo ni de cocina. Esta categoría sí incluye personas u organizaciones que promueven el terrorismo. También incluye sitios relacionados con armas, municiones y artículos para artes marciales y defensa personal (por ejemplo, pulverizadores, puños americanos), así como artículos de coleccionismo afines.



Drogas y medicamentos: sitios web que fomentan el consumo de drogas o facilitan contactos / lugares donde poder adquirirlas. Incluye sitios que venden directamente medicamentos bajo receta sin supervisión de un médico. No se incluyen sitios informativos / preventivos sobre drogas.

Hackers: sitios web en los que es posible encontrar software ilegal, así como información para acceder ilícitamente a sistemas informáticos, dispositivos de hardware u ordenadores personales (intrusión).

Modelos: sitios web que contienen fotografías de modelos; aquellos sitios en los que tipo de fotos retratan modelos total o parcialmente desnudos están incluidos en la categoría de pornografía.

Racismo: sitios web de contenido abiertamente xenófobo o que incitan a comportamientos racistas por motivos de cultura, raza, orientación sexual, religión, ideología, etc.

Sectas: sitios web de sectas peligrosas, como los así llamados adoradores de Satán.

Violencia: sitios web con contenidos abiertamente violentos, que incitan a la violencia o hacen apología de la misma.

Anorexia y bulimia: sitios web dedicados a promover e instigar trastornos de la alimentación.

Chat: sitios web a través de los cuales es posible comunicarse con otros usuarios en tiempo real.

Encuentros, Relaciones: Sitios web a través de los cuales es posible conocer a otras personas: búsqueda de pareja, relaciones, etc.

Juegos: sitios web en los que se puede jugar en línea o desde los cuales pueden descargarse videojuegos.

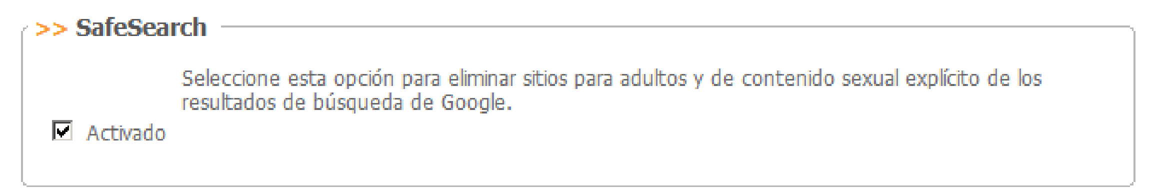
Música: sitios web desde los cuales es posible adquirir o descargar música, o bien encontrar información relativa a cantantes y grupos musicales en general.

Radio y TV por Internet: sitios web de emisoras de radio y canales de televisión. Incluyen aquellos que efectúan retransmisiones en línea.

Servidores P2P: sitios web que incluyen aplicaciones y programas P2P.

6.1.4 SafeSearch

Seleccione si desea que SafeSearch de Google (y de otros buscadores) ha de habilitarse por defecto (independientemente de lo configurado por el usuario en el propio buscador).



6.1.5 Tipos de Fichero a ser bloqueados

Aparte de filtrar categorías de páginas web, OPTENET permite el establecimiento de restricciones sobre los ficheros que pueden ser descargados. Especifique aquellas extensiones de ficheros a bloquear.



Existirán dos listas:

- Ficheros cuya descarga está permitida.
- Ficheros a bloquear.

Por defecto, todo tipo de fichero estará permitido.

En ambas listas, los ficheros estarán organizados en "familias":

- Archivos comprimidos
- Imágenes
- Música
- Programas
- Video
- Extensiones Personalizadas. Obsérvese que bajo las listas existe una sección que permite la introducción de extensiones de ficheros adicionales a ser bloqueadas, haciendo posible el filtrado de todo tipo de ficheros.

El filtro de Optenet efectúa "Análisis del Contenido" a fin de detectar tipos de fichero aun habiendo sido renombrados con una extensión diferente. Por ejemplo, si se solicita el bloqueo de ficheros mp3 y se renombra el fichero queen.mp3 por queen.gif, el filtro detectaría el tipo real y bloquearía el fichero.



6.1.6 Horarios de Navegación



Esta sección permite el establecimiento de restricciones adicionales en el acceso a internet:

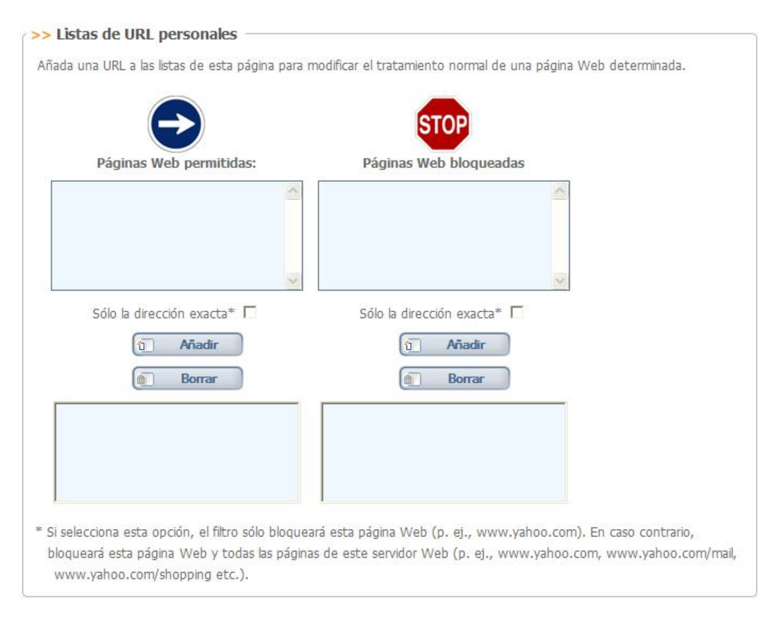
- Si los horarios no han sido activados, la navegación será permitida siempre (a cualquier hora, aplicando obviamente las restricciones de acceso a categorías prohibidas y la descarga de ficheros no permitidos).
- Si se activa el uso de horarios, Vd. podrá establecer límites de tiempo sobre el uso de Internet:
  - Podrá definir hasta tres franjas horarias por día de la Semana.

    Nota: Si no se establece ninguna franja horaria para un día de la semana, la navegación estará permitida durante todo el día (o hasta que se alcance el máximo número de horas de uso permitidas por día).
  - Máximo número de horas de navegación por día.
  - Máximum número de horas de navegación acumulada en la Semana.

  Estas restricciones de uso (Max. Número de horas/día, Max. Número de horas semanales) funcionarán independientemente de la hora del PC.

Podrá activar o desactivar el uso de horarios seleccionando las opciones “**Activado**” o “**Desactivado**”.

6.2 Listas de URLs Personales (Listas Blancas y Negras)



Será posible la creación de una Lista Blanca de URLs de confianza y de una Lista Negra de URLs a bloquear sin importar la categoría a la que pertenezcan:

- Vd. podrá personalizar el filtro de forma que ciertas páginas sean accesibles aún perteneciendo a categorías prohibidas. Éstas serán las incluidas en la lista de *Páginas Web Permitidas*.
- De forma análoga, Vd. podrá evitar que los usuarios accedan a ciertas páginas, sin importar que pertenezcan a categorías permitidas.

- Si desea permitir o bloquear una dirección exacta, marque la casilla de verificación existente a tal efecto.
- De no ser así, se bloqueará el dominio completo.
  - » Ejemplo. Si introduce www.yahoo.com y no marca la casilla "*Solo la dirección exacta*", los siguientes subdominios también serían bloqueados o permitidos según proceda:
    - www.yahoo.com/mail
    - www.yahoo.com/shooping etc

6.3 Informes (Historial de Navegación)

Vd. podrá consultar qué páginas han intentado ser visitadas por los diferentes usuarios y si el acceso ha sido permitido o bloqueado. Los informes solo mostrarán información de la navegación en aquellos periodos en los que el filtro haya permanecido activo.

En esta sección podrá:

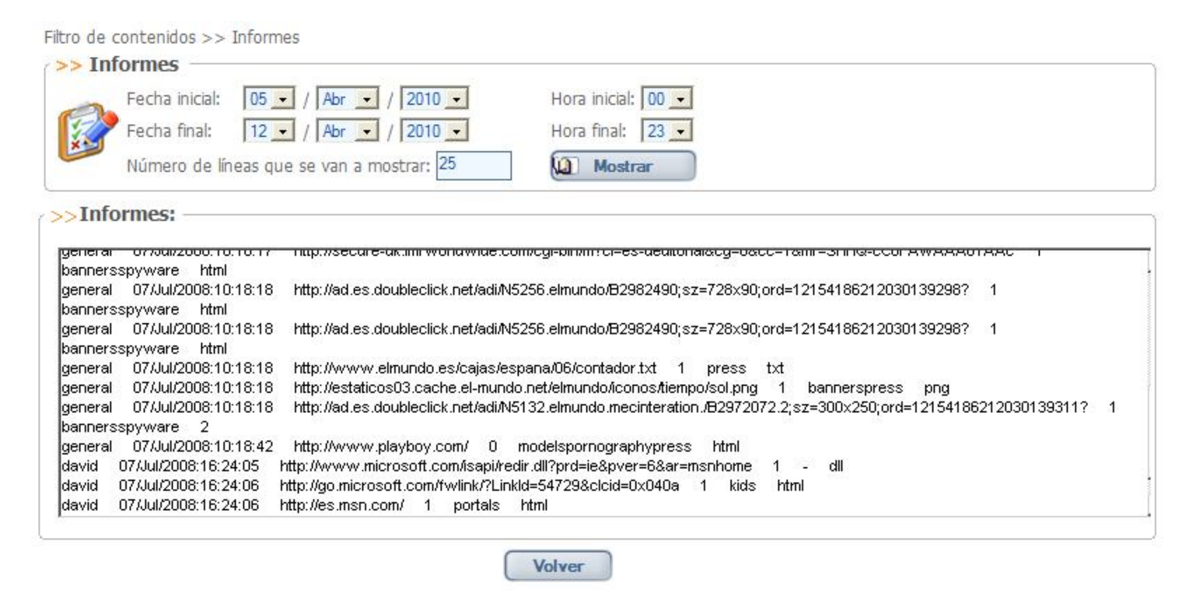
- Especificar si desea guardar información sobre las solicitudes de navegación.
  - » Marque la Casilla de Verificación [*Guardar Informes*] a fin de registrar esta información.
  - » Decida con qué frecuencia ha de borrarse la información de historial de navegación (a fin de ahorrar espacio en disco). Por defecto, será establecido a 15 días.

- Ver Informes de Navegación (información disponible en caso de que la opción [*Guardar Informes*] haya sido marcada.



Haga click en [*Ver Informes*] para establecer:

- El periodo de tiempo a Consultar (de fecha a fecha)
- Número de líneas a mostrar (número de peticiones http a mostrar):



Las líneas del informe tienen el siguiente formato:

Nombre Perfil | Fecha | hora | URL | Acceso no bloqueado (0) / Acceso bloqueado (1) | Categoría | Tipo de Fichero

6.4 Perfiles de Filtrado

Cuando diferentes usuarios utilizan el mismo PC, probablemente necesitará definir diferentes reglas para cada usuario o grupos de usuarios.

Ejemplo. Establecer diferentes restricciones para su hijo de 10 años, su hijo de 16 años y para Vd. mismo.

Un *Perfil de Filtrado* permite que el filtro de contenidos opere de forma diferente a la configuración por defecto y que tan solo aplique a ciertos usuarios.



Si no se crea ningún perfil adicional, el filtro opera utilizando la configuración por defecto que se ha descrito en apartados anteriores.

El administrador puede crear para cada miembro de la familia / de la compañía un Perfil de filtrado basado por ejemplo en su edad o puesto de trabajo.

6.4.1 Habilitando/Deshabilitando el uso de Perfiles



Los Perfiles permiten modos de filtrado personalizados al usuario que está navegando. Los Perfiles serán de utilidad cuando un mismo PC tiene más de un usuario. Por ejemplo, en familias es habitual la creación de diferentes perfiles para niños y adultos.

Para activar los *Perfiles de Filtrado*:

1) Entre en la consola de Administración.
2) Seleccione la pestaña [*Filtro de Contenidos*].
3) Seleccione la opción de menú [*Perfiles*].
4) Haga click sobre [*Habilitar Perfiles*].

Si no desea establecer medidas especiales y prefiere que todos los usuarios sean gestionados bajo las mismas restricciones de filtrado, podrá deshabilitar el uso de Perfiles. Obviamente, esto solo será posible si previamente ha habilitado el uso de Perfiles. Para deshabilitar el uso de Perfiles:

1) Entre en la Consola de Administración.
2) Seleccione la pestaña [*Filtro de Contenidos*].
3) Seleccione la opción de menú [*Perfiles*]
4) Haga Click sobre [*Deshabilitar Perfiles*].

A partir de este momento, todos los usuarios navegarán utilizando la misma configuración del filtro.

6.4.2 Creando nuevos Perfiles



Para crear un Perfil de Filtrado:

1) Entre en la Consola de Administración.
2) Seleccione la pestaña [*Filtro de Contenidos*].
3) Seleccione la opción de menú [*Perfiles*].
4) Haga click sobre el botón [*Habilitar Perfiles*].
5) Introduzca el nombre de un perfil en la caja de texto y haga click sobre el botón [*Nuevo Perfil*].
6) Aparecerá una nueva ventana donde podrá establecer para el nuevo perfil, las restricciones sobre las categorías web a visitar, ficheros que pueden ser descargados, gestión de aplicaciones etc.
7) En la parte inferior de la pantalla, puede apreciarse un listado en el que se muestran todos los perfiles existentes.

6.4.3 Configurando/Editando un Perfil

Para configurar (por primera vez) o modificar un Perfil:

1) Entre en la Consola de Administración.
2) Seleccione la pestaña [*Filtro de Contenidos*].
3) Seleccione la opción de menú [*Perfiles*].
4) Seleccione el Perfil a modificar.
5) Haga Click en el botón [*Modificar Configuración*].

6) Se mostrará una nueva ventana (indicando en la parte superior, el nombre del perfil que se va a modificar).

7) El perfil se mostrará vacio (en caso de tratarse de un nuevo perfil). En otro caso, mostrará la lista de usuarios que se hayan asignado al perfil en cuestión:



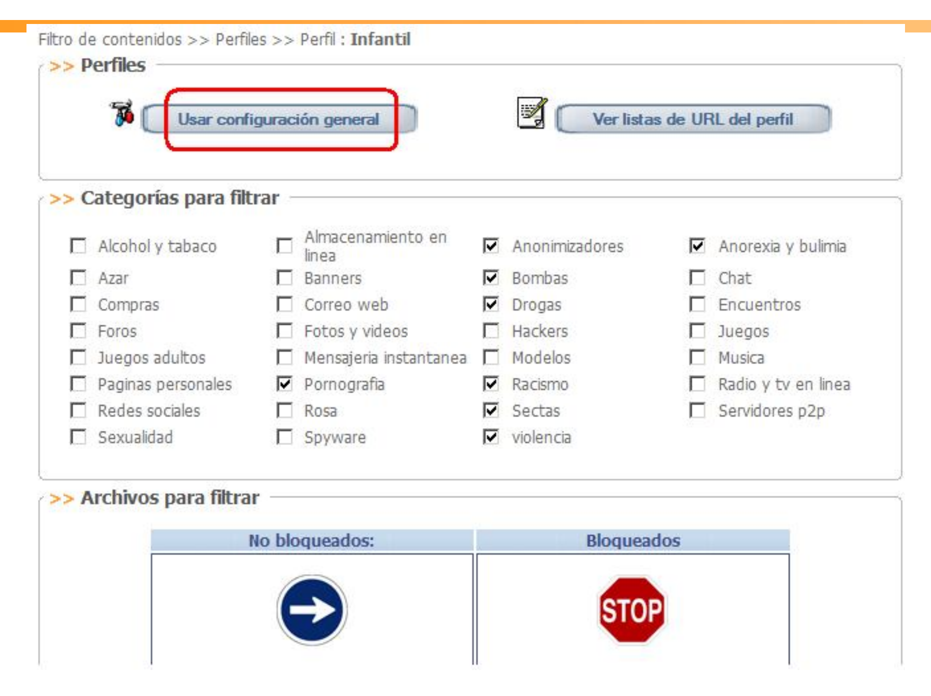
Seleccione los usuarios a ser incluidos en el perfil (en la lista de la derecha, aparecerán listados todos los usuarios de Windows y podrá pasar a la lista de la izquierda los que procedan):

8) Finalmente, será posible configurar las siguientes características de filtrado para el perfil:

- Restricciones de filtrado web (categorías de sitios web, ficheros a bloquear, horarios de navegación etc.).
- Restricciones sobre Protocolos (restricciones basadas en los protocolos de las aplicaciones: P2P, Mensajería instantánea, Correo, Grupos de noticias, Chat, Mundos Virtuales, otros).

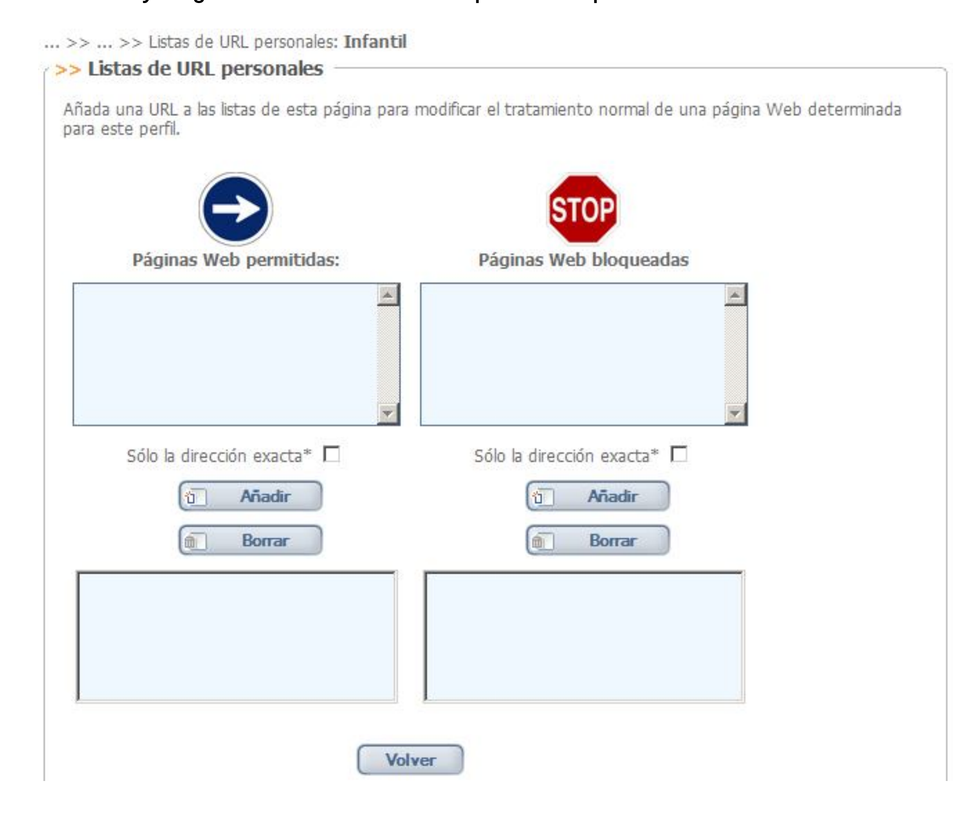
Restricciones específicas del Filtro de Contenidos:

Haga Click sobre el botón [*Filtro de Contenidos*]. Se abrirá una nueva ventana en la que configurar el tipo de filtrado de contenidos a aplicar a los usuarios de este perfil.



Haciendo Click sobre el botón [*Usar Configuración General*] se copiará la configuración general a este perfil, pudiendo añadir o eliminar restricciones.

Haga Click sobre [Ver Listas de URLs del Perfil*]* para abrir una nueva ventana en la que se puedan definir listas blancas y negras de URLs exclusivas para este perfil:



Restricciones específicas en base a los Protocolos de las Aplicaciones:



Haga Click sobre el botón [*Protocolos*]. Se mostrará una nueva ventana donde podrá configurarse las restricciones en base a los protocolos de las aplicaciones usadas. El establecimiento de este tipo de restricciones será descrito más adelante en este manual.



6.4.4 Borrando Perfiles de Filtrado

Para borrar un Perfil de Filtrado:

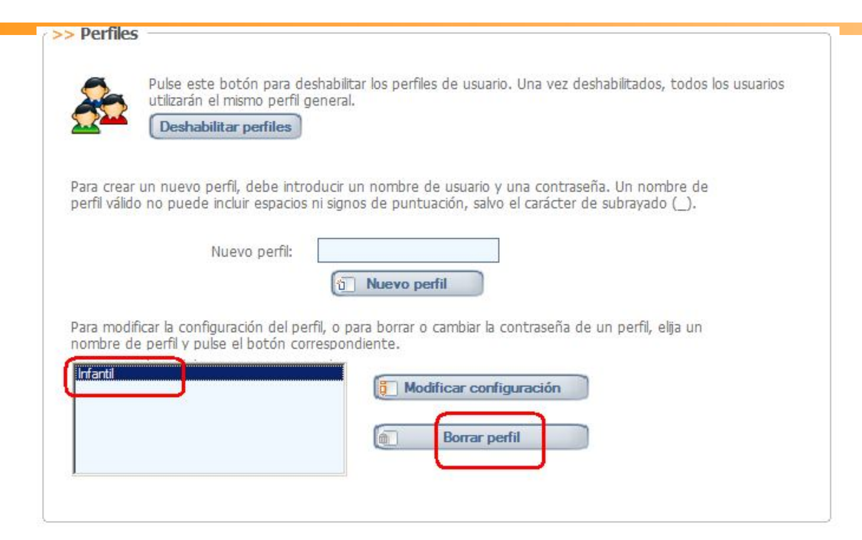
1) Entre en la Consola de Administración.

2) Seleccione la pestaña [*Filtro de Contenidos*].

3) Seleccione la opción de menú [*Perfiles*].

4) Seleccione el Perfil a eliminar

5) Haga Click sobre el botón [*Borrar Perfil*]



6.5 Contribución – Añadir Sitios web al Filtro

Contribuya con direcciones de Internet que no han sido detectadas por el filtro (URLs no incluidas en las listas de Optenet ni detectadas por el análisis de contenidos) y que Vd. considere que debieran ser incluidas en alguna de las categorías web (páginas de pornografía etc.).

El Departamento de Revisión de Optenet verificará la dirección de contribución y la asignará a la categoría correspondiente.

Cuando una página ha sido revisada, es clasificada como parte de una o más Categorías. Adicionalmente, si nos indica su correo, será informado del tipo de acción que ha sido llevada a cabo en relación con su solicitud de revisión.

A diferencia de las *Listas Personales*, la contribución informa a OPTENET sobre páginas que debieran ser filtradas en beneficio de todos los usuarios.





6.6 Configuración Avanzada

Las URLs de servidor que añada a esta lista no serán filtradas ni aparecerán en los historiales de navegación. El acceso será siempre permitido a estas páginas o servidores.

Añada aquellos Servidores que empleen aplicaciones instaladas en su ordenador para efectuar las actualizaciones automáticas de software (por ejemplo, si no está utilizando el Antivirus de Optenet, el sitio web de la actualización de su Antivirus).

Una vez efectuados los cambios, deberá reiniciar el PC para que éstos sean tenidos en cuenta.

Las páginas introducidas en esta sección son totalmente excluidas del filtrado. No aparecerán en el historial de navegación, nunca serán bloqueadas y están exentas de restricciones en base a horarios de navegación.



6.7 Filtrado de Protocolos

En esta sección podrá configurar cómo filtrar los diferentes protocolos de aplicaciones, seleccionando la acción a ser llevada a cabo en cada caso:

- Permitido – El acceso a los programas y aplicaciones que hacen uso de tal categoría de protocolos estará permitido.
- Bloqueado – El acceso a los programas y aplicaciones que hacen uso de tal categoría de protocolos será bloqueado.
- Por horario – El acceso es regulado en base a horarios (franjas horarias por día de la semana):
  - » Para aquellos días en los que se establece una o varias franjas horarias, el acceso solo estará permitido durante dichas franjas horarias.
  - » Para aquellos días en los que no se defina ninguna franja horaria, el acceso estará permitido durante todo el día.

Los protocolos (o categorías de Protocolos) disponibles serán:

- P2P
- Mensajería Instantánea

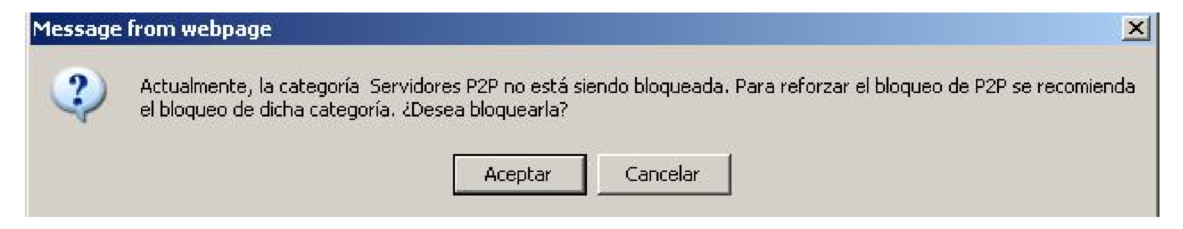
- Correo Electrónico
- Grupos de Noticias (NewsGroups)
- Chat
- Mundos Virtuales
- Otros (En base a Configuración de Puertos).



6.7.1 P2P

Esta opción permite controlar el uso de aplicaciones P2P (como por ejemplo, Emule, Gnutella, Kazaa ...) utilizadas para compartir fotos, películas, música, videos, software etc.

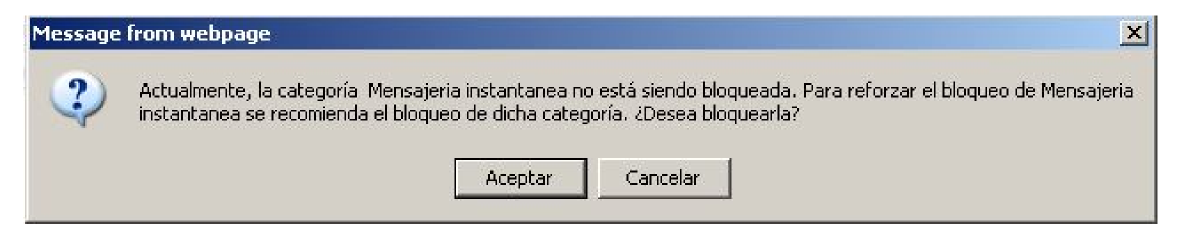
⚠ En caso de marcar el bloqueo de Protocolos P2P, si la categoría web "Servidores P2P" no ha sido marcada como una categoría a bloquear (véase [*Filtro de Contenidos* >> *Configuración*]), la herramienta le preguntará si además desea bloquear este tipo de sitios web:



6.7.2 Mensajería Instantánea

Esta opción permite controlar el uso de aplicaciones de mensajería instantánea (como por ejemplo, Microsoft MSN Messenger, Yahoo Instant Messenger, ICQ 5.0, AIM), utilizadas para el envío de mensajes y ficheros en tiempo real.

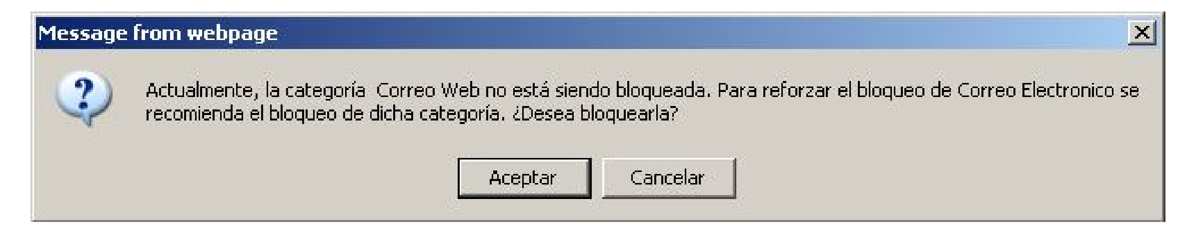
⚠ En caso de marcar el bloqueo de Protocolos de Mensajería Instantánea, si la categoría web [Mensajería Instantánea] no ha sido marcada como una categoría a bloquear (véase [*Filtro de Contenidos* >> *Configuración*]), la herramienta le preguntará si además desea bloquear este tipo de sitios web:



6.7.3 Correo Electrónico

Esta opción permite controlar el uso del correo accedido mediante los protocolos POP3 (puerto 110), SMTP (puerto 25) e IMAP (puerto 143).

⚠ En caso de marcar el bloqueo de Protocolos de Correo, si la categoría web [Correo Web] no ha sido marcada como una categoría a bloquear (véase [*Filtro de Contenidos* >> *Configuración*]), la herramienta le preguntará si además desea bloquear este tipo de sitios web:



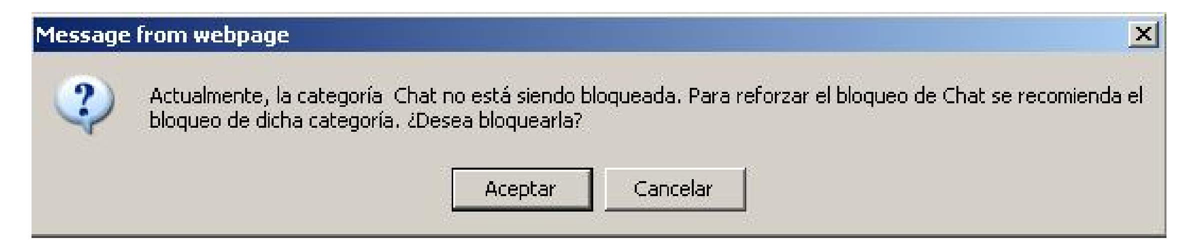
6.7.4 Grupos de Noticias (Newsgroups)

Esta opción permite controlar el uso de grupos de noticias (por ejemplo, NNTP), utilizados como foros de discusión donde los usuarios pueden intercambiar opiniones.

6.7.5 Chat

Esta opción permite controlar el uso de aplicaciones de Chat (como por ejemplo, IRC), a través de las cuales los usuarios pueden chatear.

⚠ En caso de marcar el bloqueo de Protocolos de Chat, si la categoría web [Chat] no ha sido marcada como una categoría a bloquear (véase [*Filtro de Contenidos* >> *Configuración*]), la herramienta le preguntará si además desea bloquear este tipo de sitios web:



6.7.6 Mundos Virtuales

Esta opción permite controlar el uso de los juegos de internet de Mundos Virtuales (como por ejemplo Second Life) donde los usuarios pueden convivir e interactuar vía avatares.

Adicionalmente, habilitando la casilla de verificación de *Configuración Avanzada*, se podrán especificar una lista de excepciones de URLs / direcciones que pueden ser permitidas o bloqueadas tal y como se detalla:

- » Se permite el uso de Mundos Virtuales y no se introduce ninguna dirección en la lista de configuración avanzada: Se permite el acceso a todas las direcciones del Mundo Virtual.
- » Se bloquea el acceso a los Mundos Virtuales y no se introduce ninguna dirección en la lista de configuración avanzada: Se bloquea el acceso a todas las direcciones del Mundo Virtual.
- » Se permite el uso de Mundos Virtuales y se añaden direcciones en la lista de configuración avanzada: Solo se permite el acceso a las direcciones incluidas en la lista.
- » Se bloquea el acceso a los Mundos Virtuales y se añaden direcciones a la lista de configuración avanzada: Solo se bloquea el acceso a las direcciones incluidas en la lista.



6.7.7 Otros

Esta opción es utilizada para establecer el comportamiento por defecto (bloqueo o acceso) sobre aquellos puertos no incluidos en la configuración de las pestañas anteriores.

Opciones:

- » Bloquear todos los demás puertos, indicando una lista de excepciones.

  O bien

- » Permitir todos los demás puertos, indicando una lista de excepciones.



6.8 Reforzando el bloqueo

A veces, existe un paralelismo entre las categorías web y las familias de protocolos que se deseen bloquear:

Protocolo	Categoría Web
P2P	Servidores P2P
Mensajería Instantánea	Mensajería Instantánea
Correo Electrónico	Correo Web
Chat	Chat
etc.	

Debido a este motivo, siempre que configure el filtro para bloquear cualquiera de dichas categorías web, la herramienta preguntará si además desea bloquear los protocolos relacionados, reforzando de esta forma el bloqueo (siempre y cuando dichos protocolos no hubieran sido ya marcados para su bloqueo).

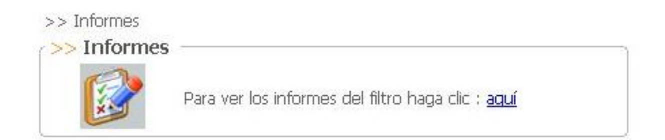
De forma análoga, siempre que bloquee un protocolo dado, si la categoría web relacionada no está prohibida, la herramienta preguntará si desea además bloquear los sitios web pertenecientes a dicha categoría.

Ejemplo. Si Vd. desde que los usuarios de un determinado perfil no puedan utilizar aplicaciones basadas en protocolos de correo, se le preguntará si además desea bloquear las páginas de correo web.



7 INFORMES

Desde esta sección podrá examinar las medidas de filtrado llevadas a cabo por la Suite de Seguridad de OPTENET.



Podrá obtener informes sobre la actividad del

- Filtro de Contenidos



8 INFORMACIÓN DE CONTACTO



Haga Click sobre el botón [*Contacto*]. Se mostrará una nueva ventana donde se informará de las cuentas de correo a la que puede dirigir:

- Peticiones relacionadas con Atención al Cliente.
- Peticiones relacionadas con Soporte técnico.



9 DESINSTALACIÓN

Para desinstalar la Suite de Seguridad de OPTENET, basta con utilizar el menú accesible desde el botón [Inicio] de su equipo. Durante el proceso de desinstalación se le solicitará la contraseña de Administración evitando de esta forma que cualquier otro usuario pueda desinstalar el programa.

IMPORTANTE: No intente desinstalar el programa eliminando los directorios y archivos de la Security Suite, ya que esto podría dañar la instalación de forma irreparable y perder totalmente el acceso a internet. Utilice siempre el acceso directo de su equipo para desinstalar el software.

Si se ejecuta la instalación de OPTENET Security Suite sobre un PC en el que el software ya estuviera instalado, se iniciará el proceso de desinstalación de la versión existente (una vez se haya introducido la contraseña de administración indicada para dicha instalación).